iSpirit 3026 交换机快速配置指南

(软件版本：iSpirit3026　1V12.img)

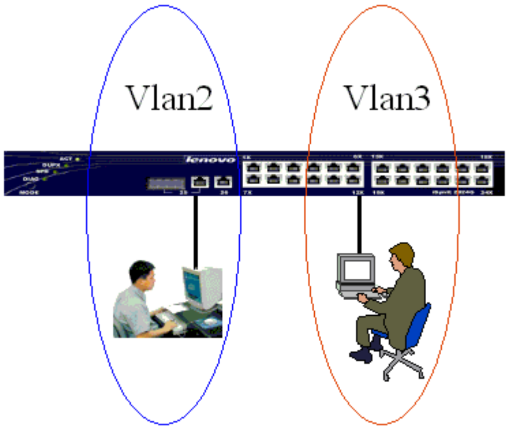
（Version 1.0）

联想网络行业方案处

2004 年 12 月

目录

一．基于 PORT（端口）的 VLAN 配置



1．网络需求

有两个用户，用户 1 和用户 2，两个用户由于所使用的网络功能和环境不同，需要分别处于不同的 VLAN 中。用户 1 在 VLAN2，连接端口 2；用户 2 在 VLAN3，连接端口 3。

2．配置步骤

Switch# vlan 2　　// 创建 vlan 2

Vlan 2 added

Switch(vlan-2)#exit

Switch# vlan 3　　// 创建 vlan 3

Vlan 3 added

Switch(vlan-3)# vlan 2　　// 在创建 vlan 2 之后,就可在配置模式下 输入 vlan 2 ，进入 vlan 2 的配置模式

Switch(vlan-2)# untag 2　　// 将端口 2 加入 vlan 2,如果还有其它端口要加入 vlan 2，那么在 vlan 2 模式下，untag x （x 为其它端口号）

Switch(vlan-2)# vlan 3　　//进入 vlan 3 配置模式

Switch(vlan-3)# untag 3　　//将端口 3 加入 vlan 3，如果还有其它端口要加入 vlan 3，那么在 vlan 3 模式下，untag x （x 为其它端口号）

3.排错

如果配置后，发现不同 VLAN 之间的 PC 机不能通信，那是正常现象，因为不同 VLAN 之间要进行通信，必须要经过三层的路由转发。

如果同一 VLAN 内的 PC 机不能进行通信，须作以下验证：

1）查看整体有哪些 VLAN

```
Switch# show vlan

-----------------------------------------------
|VID |Name                              | Status |
|----+-------------------------------+--------|
|1    |Default VLAN 1                  | Static |
|---------------------------------------------|
|2    |vlan2                           | Static |
|---------------------------------------------|
|3    |vlan3                           | Static |
|---------------------------------------------|
```

// 如果这里得到的信息不是 vlan 2 和 vlan 3 的信息，那么就要重新设置。

2） 看设置的端口是否在相应的 VLAN 内，并且是以“U”的形势加入的

Switch# show vlan 2 //查看 vlan 2 的配置

```
Vlan 2 Port Map
(-=None, M=Tagged, U=Untagged)
                        (-=None, M=Member, F=Forbidden, U=Untagged)
------------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|               |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|---------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |-|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
------------------------------------------------------------------
```

// 查看 vlan 2 ，发现端口 2 标记为 “U”，说明配置正确。 如果 U 不是标记在 2 处，那么就是配置有问题，要重新配置。

Switch# show vlan 3 //查看 vlan 3 的配置

```
Vlan 3 Port Map
(-=None, M=Tagged, U=Untagged)
                        (-=None, M=Member, F=Forbidden, U=Untagged)
------------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
```

```
|                |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|----------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration  |-|-|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|
---------------------------------------------------------------------
```

// 查看 vlan 3 ，发现端口 3 标记为 “U”，说明配置正确。如果 U 不是标记在 3 处，那么就是配置有问题，要重新配置。

3） 查看特定端口，端口的 pvid 号必须和端口所在 vlan 的号码一致

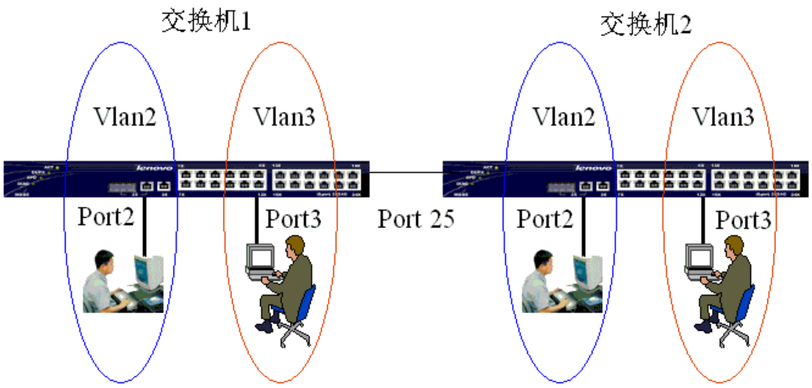
如例，端口 2 在 vlan 2 中，端口 2 的 pvid 号应该为 2 。

```
Switch# show port 2

Port                 :  2
ifIndex              :  0x2100002
Admin State          :  Enable
Set Speed            :  autonegotiate
Actual Speed         :  unknown
Link                 :  Down
Ingress Filter       :  Disable
Flow Control         :  Disable
PortVlanID           :  2    //端口 2 的 pvid 号为 2，配置正确
PortDefaultPriority  :  0

Switch# show port 3
Port                 :  3
ifIndex              :  0x2100003
Admin State          :  Enable
Set Speed            :  autonegotiate
Actual Speed         :  full-100
Link                 :  Up
Ingress Filter       :  Disable
Flow Control         :  Disable
PortVlanID           :  3    //端口 3 的 pvid 号为 3，配置正确
```

二．基于 802.1Q 的 vlan 配置



1.网络需求

有两台 iSpirit3026 交换机分别连接两个用户。用户 1 和 3 属于 vlan 2，用户 2，4 属于 vlan 3。详细情况如下：

用户	所属 VLAN	连接端口	所属交换机	级联端口
用户 1	Vlan2	2	交换机 1	25
用户 2	Vlan3	3	交换机 1	25
用户 3	Vlan2	2	交换机 2	25
用户 4	Vlan3	3	交换机 2	25

2．配置步骤

交换机 1：

```
witch# vlan 2
  Vlan 2 added
Switch(vlan-2)# untag 2
Switch(vlan-2)# tag 25
Switch(vlan-2)# exit

Switch# vlan 3
  Vlan 3 added
Switch(vlan-3)# untag 3
Switch(vlan-3)# tag 25
Switch(vlan-3)# exit
```

交换机 2：

```
witch# vlan 2
```

```
  Vlan 2 added
Switch(vlan-2)# untag 2
Switch(vlan-2)# tag 25
Switch(vlan-2)# exit

Switch# vlan 3
  Vlan 3 added
Switch(vlan-3)# untag 3
Switch(vlan-3)# tag 25
Switch(vlan-3)# exit
```

3.排错

跨交换机的 vlan，在同一个 vlan 内的 pc 机都能够通信的，如果不能通信，需要查看的信息如下：

1、连接 pc 机的端口是以 " u " 模式加入这个 vlan 的，并且端口的 pvid 号和 vlan 号应该一致。
2、级联端口是加入到每一个 vlan 中的，并且在每一个 vlan 内都是以"M"模式加入的，并且端口的 pvid 号为 1。

查看交换机 1 的配置

```
Switch# show vlan     //查看整体 vlan 的配置

------------------------------------------------
|VID |Name                                | Status |
|----+--------------------------------+--------|
|1    |Default VLAN 1                   | Static |
|----------------------------------------------|
|2    |vlan2                            | Static |
|----------------------------------------------|
|3    |vlan3                            | Static |
|----------------------------------------------|


Switch# show   vlan 2     //查看 vlan 2 的配置

Vlan 2 Port Map
(-=None, M=Tagged, U=Untagged)
                          (-=None, M=Member, F=Forbidden, U=Untagged)
 -----------------------------------------------------------------------
|  Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
```

```
|              |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|--------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |-|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|M|-|
-------------------------------------------------------------------
```

// 查看 vlan 2 ，发现端口 2 标记为 “U”，端口 25 标记为 “M”， 说明配置正确。 如果 U 不是标记在 2 处，那么就是配置有问题，要重新配置

Switch# show vlan 3 //查看 vlan 3 的配置

Vlan 5 Port Map
(-=None, M=Tagged, U=Untagged)
(-=None, M=Member, F=Forbidden, U=Untagged)

```
-------------------------------------------------------------------
| Port Number  |0|0|0|0|0|0|0|0|0|1|1|1|1|1|1|1|1|1|1|2|2|2|2|2|2|2|
|              |1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|7|8|9|0|1|2|3|4|5|6|
|--------------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
| Configuration |-|-|U|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|-|M|-|
-------------------------------------------------------------------
```

注意交换机的端口 2 的 pvid 号为 2，端口 3 的 pvid 号为 3，级联端口 25 的 pvid 还是为 1。查看端口状态（包行 pvid 信息）的命令为：swtich# show port x （x 为端口号）。

查看交换机 2 的配置

由于在本案例中，交换机 2 的配置和 交换机 1 的配置是一样的，所以查看配置方法和结果应该是一样的。如果不一样，就要重新配置一下。

三．私有 vlan 配置

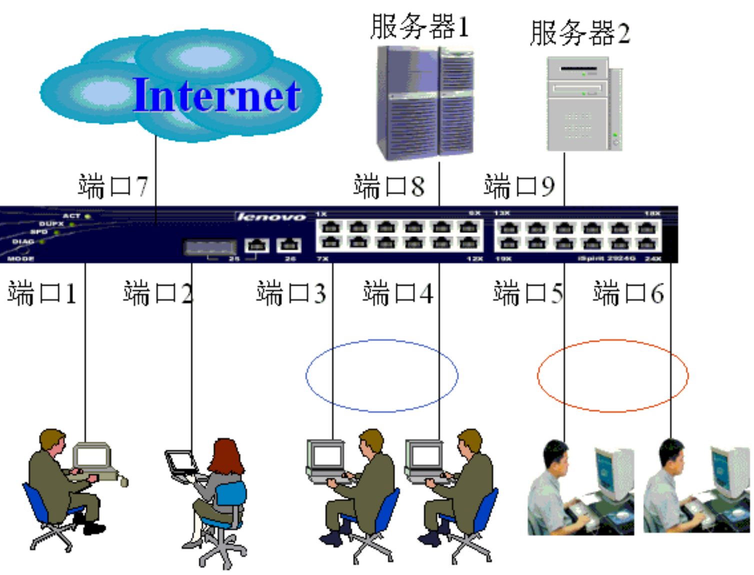
1.私有 vlan 配置案例一

1.1 网络需求

用户1 和用户2 只能访问服务器1、服务器2 和互联网，用户1 和用户2 之间不能通信，用户1 和用户2 不能与用户3 到6 通信。用户3 和用户4 可以访问服务器1、服务器2 和互联网，用户3 和用户4 之间可以通信，用户3 和用户4 不能与用户1 到2、用户5 到6 通信。用户5 和用户6 可以访问服务器1、服务器2 和互联网，用户5 和用户6之间可以通信，用户5 和用户6 不能与用户1 到4 通信。服务器1 和服务器2 可以和用户1 到6 通信，可以访问互联网，服务器1 和服务器2 之间可以通信。

通过私有vlan技术，可以将上述复杂的网络需求，在iSpirit3026交换机进行简单配置就可以实现。

配置规划如下图：端口1-9 属于一个私有VLAN 组，端口1 和端口2 是隔离端口，端口3、4、5 和6 是共用端口，其中端口3 和4 是一个共用端口组，端口5 和6 是一个共用端口组，端口7、8 和9 是混杂端口。



1.2 配置步骤

Switch# private 1　　　　　//进入私有vlan 的配置模式，并创建私有vlan 1

// 注意：

iSpirit 3026最多支持12个私有vlan，私有vlan号的范围 1~ 12。

Switch(privatevlan-1)# vlan 2 6 2　　//配置私有vlan 包含的vlan 范围

// 注意：

*这里为什么要设置为 2（最小数） 6（最大数） 2 （私有vlan 1中的主vlan号）？这是因为在本案例中，我们要设置2个隔离端口，2个公共端口组，总共就是4，所以需要使最大数减去最小数等于或者大于4，但不能大于26。这里的最小数2，并不一定要用2，也可以用其它数，但不能超过4096。只要保证最大数减去最小数等于或者大于4，且不大于26就可以。主vlan号，就是要包含在最大数和最小之间的任一个，一般都是选择最小那个，在本案例中，我们选择了2。如果要设置5个隔离端口，1个混杂端口，那么总共就是6，那么最大数减最小数的值同样要满足上述的条件。例如：*Switch(privatevlan-1)# vlan 10 16 10

如果配置了私有vlan之后，还要设置普通的vlan，例如：基于端口或者基于802.1Q的vlan。那么这些vlan的vlan号是不能和私有vlan中的vlan号重叠。例如：本例中，私有vlan中的vlan号包含了10～16，所以创建其它普通vlan时就不能用到这些vlan号。

```
Switch(privatevlan-1)# isolate 1-2    //配置隔离端口1，2
Switch(privatevlan-1)# community 1 3-4    //配置公共端口组1 ，包含端口3，4
Switch(privatevlan-1)# community 2 5-6    //配置公共端口组2 ，包含端口5，6
```

//注意：

在每个私有vlan里，最多可以有6组公共端口组，公共端口组的范围为1~6

```
Switch(privatevlan-1)# promiscuous 7-9    //配置混杂端口
Switch(privatevlan-1)# enable    //启用私有vlan；
```

// 注意：

*当要修改私有vlan 配置时，必须使用**disable**命令关闭私有vlan,否则，无法修改私有vlan的配置*

```
Switch# show privatevlan 1  //查看私有vlan 1 配置信息
Private vlan group : 1
status : active
max vlan number : 6
min vlan number : 2
primary vlan number : 2
promiscuit port : 7 8 9
iSolatePort port : 1 2
community 1 port : 3 4
community 2 port : 5 6
```

1.3 排错

如果配置不成功可能有以下几个原因：

1、min-vlanid 值比max-vlanid 大。

2、primary-vlanid 不在min-vlanid 到max-vlanid 范围内。

3、max-vlanid 值减min-vlanid 大于26。
4、min-vlanid 值到max-vlanid 的VLAN范围有至少一个VLAN被普通VLAN占用。
5、私有VLAN 组与其它的私有VLAN 组有VLAN 范围重叠的现象。
6、如果该私有VLAN 组处于生效（active）状态，就不能够对该私有vlan 做任何配置
7、私有VLAN 所包含的vlan 数至少应该大于等于私有vlan 的（私有端口个数+ 公用端口组数+1）
8、私有VLAN 组内没有混杂端口。
9、私有VLAN 组内既没有隔离端口又没有共用端口组。
10、私有VLAN 组内混杂端口、共用端口和隔离端口有重叠的现象。
11、私有VLAN 组与其它的私有VLAN 组有混杂端口、共用端口和隔离端口重叠的现象。
12、如果私有VLAN组内的混杂端口、共用端口或隔离端口属于普通VLAN的untagged 成员，则要从该普通VLAN中清除这些端口，是这些端口不属于该普通VLAN的成员

1.4 附件

私有 VLAN 端口通信关系

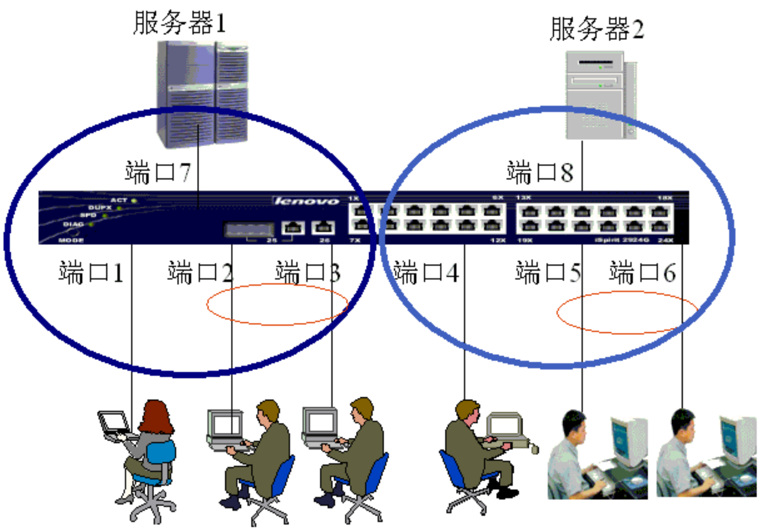
	混杂端口	组 1 共用端口	组 2 共用端口	隔离端口
混杂端口	可以	可以	可以	可以
组 1 共用端口	可以	可以		
组 2 共用端口	可以		可以	
隔离端口	可以			

2.私有 vlan 配置案例二

2.1 网络需求

配置两个VLAN组

如下图所示是两个私有VLAN组的例子，私有VLAN组1 包括端口1-3 和端口7，私有VLAN组2 包括端口4-6 和端口8。在私有VLAN 组1 中，端口1 是隔离端口，端口2 和3 是共用端口，端口2 和3 组成一个共用端口组，端口7 是混杂端口。在私有VLAN 组2 中，端口4 是隔离端口，端口5 和6 是共用端口，端口5 和6 组成一个共用端口组，端口8 是混杂端口。在私有VLAN 组1 中，用户1 只能与服务器1 通信，用户1 不能与用户2 到3 通信，用户2 和用户3 可以与服务器1 通信，并且用户2 和用户3 能够互相通信，但不能与用户1 通信。在私有VLAN组2 中，用户4 只能与服务器2 通信，用户4 不能与用户5 到6 通信，用户5 和用户6 可以与服务器2 通信，并且用户5 和用户6 能够互相通信，但不能与用户4 通信。



2.2 配置步骤

配置私有vlan 1

```
Switch# privatevlan 1
Switch(privatevlan-1)# vlan 1000 1002 1000
Switch(privatevlan-1)# isolate 1
Switch(privatevlan-1)# community 1 2-3
Switch(privatevlan-1)# promiscuous 7
Switch(privatevlan-1)# enable
```

查看私有vlan 1 的配置信息

```
Switch# show privatevlan 1
Private vlan group : 1
status : active
max vlan number : 1002
min vlan number : 1000
primary vlan number : 1000
promiscuit port : 6
iSolatePort port : 1
community 1 port : 2 3
```

配置私有vlan 2

```
Switch# privatevlan 2
Switch(privatevlan-1)# vlan 2000 2002 2000
Switch(privatevlan-1)# isolate 4
Switch(privatevlan-1)# community 1 5-6
Switch(privatevlan-1)# promiscuous 8
Switch(privatevlan-1)# enable
```

查看私有vlan 2 的配置信息

```
Switch# show privatevlan 2
Private vlan group : 2
status : active
max vlan number : 2002
min vlan number : 2000
primary vlan number : 2000
promiscuit port : 8
iSolatePort port : 4
community 1 port : 5 6
```

2.3 排错 （请参阅第1个例子的排错方法）

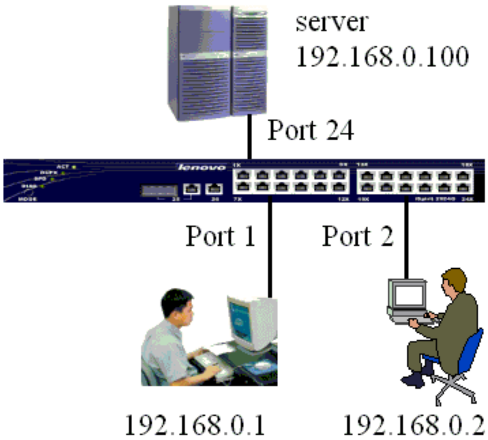
注：私有VLAN组1 中的设备要和私有VLAN组2 中的pc相互通信必须通过三层转发。

附 :有关私有vlan介绍、配置命令等相关详细资料，请到http://www.lenovonetworks.com下载相关用户手册。

四. Vlan 内端口隔离配置

1.网络需求

有两个用户在同一个 vlan 内（默认为 vlan1），为了每个用户的相对独立保密的情况下，需要同一个 vlan 内的任意两个用户不能够相互访问，但是用户的端口都需要通过级联端口 24 向上访问网络。这种需求可以通过 vlan 内的端口隔离的功能来实现。



2.配置步骤

1）将端口 1 和 2 设置为隔离端口，但可以通过端口 24 进行上联访问。

```
Switch# port 1
Switch(port 1)# separated  24
Switch# port 2
Switch(port 2)# separated  24
```

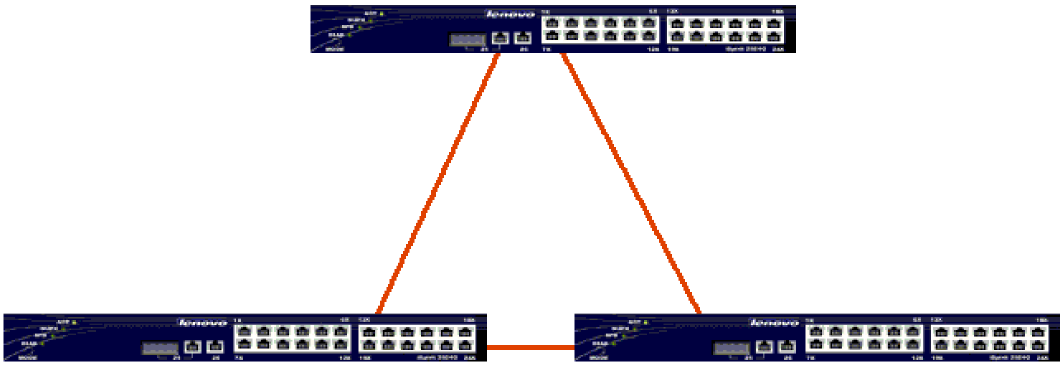
2）查看配置信息

```
Switch# show separated
Port                 Egress Port              Status
   1                         24              Separated
   2                         24              Separated
   3                        N/A              unSeparated
   4                        N/A              unSeparated
```

五. STP（生成树）配置

1.网络需求

为了避免三台 iSpirit3026 连接在一起构成环路，需要配置 STP（生成树协议）。



2.配置步骤

1） 在全局模式下启用 stp 协议

Switch# stp   //在交换机上启用 STP，默认情况下交换机在全局上是关闭 STP，但是各个端口默认情况下是启用 STP。（端口启用 STP，但是交换机全局下没有启动 STP，端口的 STP 是没有生效的）

2) 确认生成树协议在每一台交换机上是打开的

```
Switch# show switch
 Ip Address        : 192.168.0.1
 Subnet Mask       : 255.255.255.0
 Default Gateway   : 0.0.0.0
 MAC Address       : 00:40:47:00:99:55
 Spanning Tree     : Enable
 IGMP Snooping     : Disabl
```

上述的 Spanning Tree 是 Enable，说明 stp 协议已经启用。

如果需要关闭生成树协议的运行，需要输入命令

Switch# no stp

生成树协议的高级命令：

设置其中第一台交换机为根交换机，需要设置他的桥优先级比其他两个桥的优先级要小，默认优先级为 32768

Switch# stp bridge priority

```
instance id(1-255): 1      //1-255 为实例号，对于简单的需求，一般只用到一个实例。
                             本例中，我们设置实例为 1，接着就是设置桥的优先级。
 Switch# stp bridge priority  A        stp bridge priority (0=<A<=65535)
```

使交换机的某个端口不参与生成树的运行，需要关闭端口的生成树功能

```
Switch# disable stp ports  portnumber     port number (1=<A<=26)
```

//在默认情况下，不管在全局模式下是否启用了 stp，所有端口都是启动了生成树功能。

3. 排错

1）察看哪一个交换机被选为根网桥：

```
Switch# show stp bridge
instance id(1-255):     1  //假设实例号为 1，那么在这里就把参数设置为 1
--- Designated Root Information ---
 Priority                  : 32768
 MAC Address               : 00:40:47:00:99:55
 Hello Time                : 2s
 Forward Delay             : 15s
 Max Age                   : 20s

 --- Bridge STP Information ---
 Bridge Priority           : 32768
 MAC Address               : 00:40:47:00:99:55
 Root Path Cost            : 0
 Root Port                 : 0
 Bridge Hello Time         : 2s
 Bridge Forward Delay      : 15s
 Bridge Max Age            : 20s
```

2）察看生成树中交换机的端口状态：

```
Switch# show stp  port  portnumber     port number (1=<A<=26)
instance id(1-255):     1
 --- Port Information ---
 STP Port                  : Enable
 Port ID                   : 1
 Priority                  : 128
 State                     : Disabled
 Path Cost                 : 19
 Designated Cost           : 0

 --- Designated Root Information ---
 Priority                  : 32768
 MAC Address               : 00:40:47:00:99:55
```

```
--- Designated Port Information ---
Port ID                   : 1
Priority                  : 128

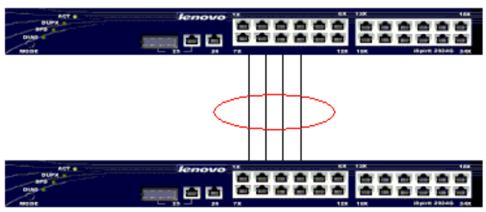
--- Designated Bridge Information ---
Priority                  : 32768
MAC Address               : 00:40:47:00:99:55
```

六. Trunk 端口聚合配置

1. 网络需求

为了增加两台 iSpirit3026 连接间的带宽，同时提供冗余功能，保证其中一条链路出了问题时，其它链路都可以正常使用，因此，在这里使用了 trunk 配置。

在交换机 1 和交换机 2 之间做 trunk 链路，各自捆绑 1-4 端口做链路聚合。



2.配置步骤

在每个交换机上执行：

Switch# trunk <cr> set trunk configuration

Switch# trunk

trunk_Id: 1 // trunk 的 ID 号，ID 号范围：0-5

trunk_Rtag: 1 //trunk 的 tag 号，tag 号范围：1-6

ports_list: 1-4 //加入 trunk 组的端口号

//注意:

配置 trunk 时，两边交换机的端口数量要一致，速度、双工等端口参数都要完全一致，但不必两边的端口号一一对应。iSpirit3026 最多支持 6 组 trunk，每组 trunk 最多可以包含 8 个 100M 端口，或者 2 个 1000M 端口。

3. Trunk 删除命令

删除一个 trunk 组

Switch# no trunk A trunk indentifier(0<=tid<=5)

4.排错

1） 如果 trunk 没有起作用，需要查看以下状态，检查所配置的 trunk 是否激活，包含的端口数量和端口号是否正确。

Switch# show trun

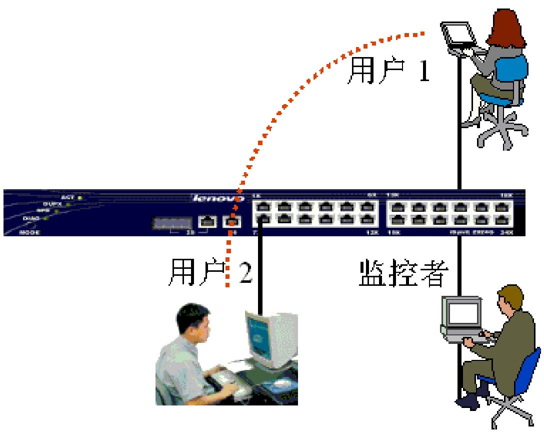
TGID	RTAG	status	Ports
0	0	Not_ready	0x00000000(none)
1	**1**	**Active**	**0x0000001e(fe1-fe4)**
2	0	Not_ready	0x00000000(none)
3	0	Not_ready	0x00000000(none)
4	0	Not_ready	0x00000000(none)
5	0	Not_ready	0x00000000(none)

2） 加入 trunk 组的几个端口一定要属于同一个 vlan，速率，双工等端口属性都要设置一样。

七. Mirror （端口镜像）配置

1.网络需求

在一台交换机中，用户 1 和用户 2 正在通信，正常情况下其他端口的用户是无法获取其通信信息的，为了检测数据流是否正常，监测者需要获取其数据流，就要用到端口镜像问题。用户 1 连接到端口 1，用户 2 连接到端口 2，监测者连接在端口 8，使监测者能够捕捉到其数据流。



2.配置步骤

Switch# mirror
Mirror Port: 8 //监控者的端口
Egress ports_list: 1 2 //被监控者出口流量的端口
Ingress ports_list: 1 2 //被监控者入口流量的端口

3.排错

1) 不要把镜像端口和被镜像端口搞反了。
镜像端口是 mirror ports,指的是观测者所在的端口
被镜像端口是 Egress ports（外出数据流），Ingress ports （进入数据流），指的是被观测的端口

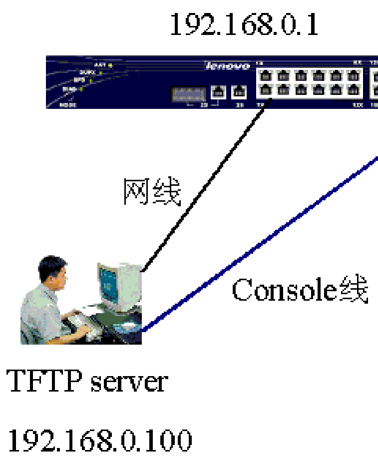
2) 用 show mirror 命令进行确认
Switch# show mirror
Mirror Mode: L2
Mirror Port: 8
Egress ports_list: 1 – 2
Ingress ports_list: 1 – 2

八．Configuration 文件备份

1．网络需求

1) 把交换机的配置文件上传（备份）到 TFTP 服务器上；
2) 把存放到 TFTP 服务器上的配置文件下载到交换机

网络拓扑图如下：



2．配置步骤

1) 设置 TFTP 服务器的 IP 地址为 192.168.0.100 iSpirit3026 交换机的 IP 地址为 192.168.0.1,并确保 TFTP 和交换机的 IP 之间能够相通

交换机 ip 地址的配置如下：

switch>enable

switch#ip add 192.168.0.1 255.255.255.0

2) 在 pc 上打开 TFTP 服务器

3) 把交换机的配置文件上传（备份）到 TFTP 服务器上,具体操作如下，在交换机上执行

Switch# upload configuration 192.168.0.100 文件名

uploading configuration ......

4) 如果为了方便，不想重新配置交换机，那么可以把保存在 TFTP 服务器上的配置文件向下传到交换机上，具体操作如下，在交换机上执行

Switch# download configuration 192.168.0.100 文件名

Do you wish to continue? [Y/N]: y

3.排错

如果上传或者下载文件不成功，需要注意以下几个方面：

1) tftp 服务器和交换机之间的 IP 是一定要相互能通。

2) tftp 服务器的 tftp 服务一定要打开。
3) 在交换机上执行的下传或下载配置文件的命令一定要写正确，特别是配置文件的名字一定要正确，区分大小写。

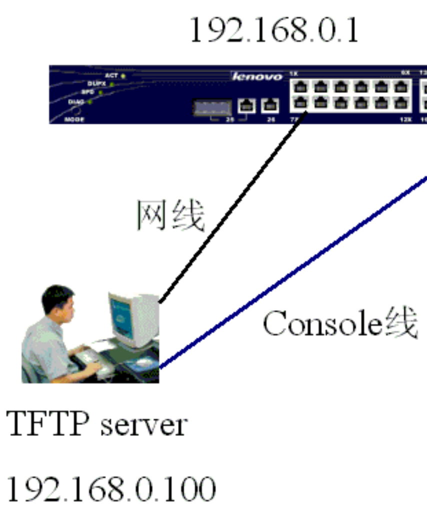
准备好的配置文件一定要放置到 tftp 服务器指定的目录下。

九．IMAGE 软件升级

1．网络环境

硬件：交换机，计算机，串口线，网线。

软件：windowns 操作系统，TFTP 服务器软件（tftpd32.exe 或者其它 tftp 软件）



2．配置步骤

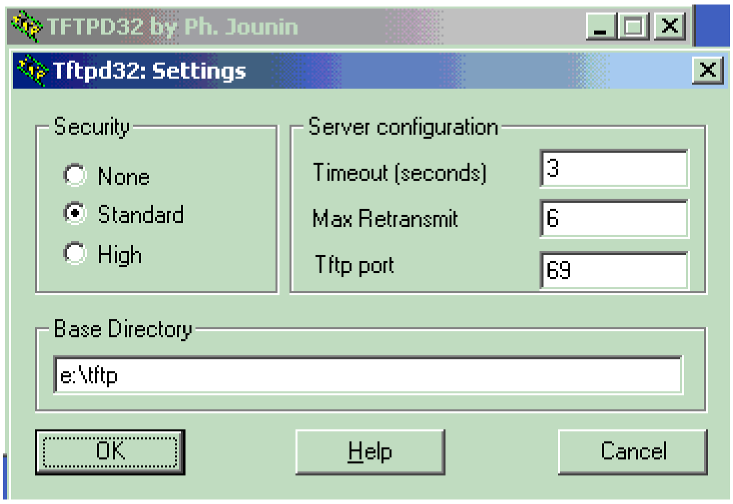
1) 配置交换机的 ip 地址

Switch>enable

Switch#ip add 192.168.0.1 255.255.255.0

Switch#show switch //可以看到刚才配置的 ip 地址

2) 设置 pc 机的 ip 地址为 192.168.0.100 ，并运行 tftp 软件。



上述 e:\tftp 为升级文件所在的位置（即升级文件存放在 e:\tftp 目录下），可以根据实际情况进行设置。

3) 在超级终端下，输入 download 命令，开始下载镜像文件。

Switch# download image 192.168.0.100 iSpirit30261V12.img
  Do you wish to continue? [Y/N]: y
  Don't Shut down power until completed!
  downloading image ......

一直等到交换机提示升级完成，然后才能重新启动交换机

注意：在升级交换机的过程中，不能断电。如果中途断电，很可能造成交换机损坏。

3．排错

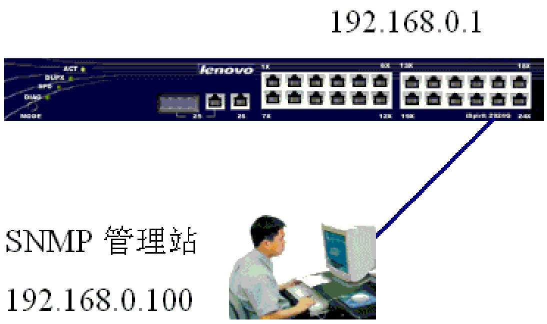
交换机映像文件升级不成功，需要查找以下几个原因：

1) 交换机和 TFTP 服务器之间是否 IP 能够通信。
2) TFTP 服务器是否正常启动，并且启动所用的 IP 地址就是交换机所能够 PING 通的。
3) 映像文件是否放到了 TFTP 服务器所指定的特定位置。
4) 在交换机上执行升级映像文件时，映像文件的名字一定不要写错。

十．snmp 配置

1.网络需求

有一个 SNMP 管理站上面运行 SNMP 管理软件，管理站的 IP 地址为 192.168.0.100。现在，管理站要管理其中一台 IP 地址为 192.168.0.1 的交换机。由于该工作站有两个管理者，一个管理者只有对交换机有查看信息的权限，另一个管理者可以对交换机进行设置。因此。在交换机上打开 SNMP 后（默认是打开的），配置了 snmp 的 community ，一个为只读，另外一个为读写。其中，只读的 community 设置为 public，读写的 community 设置为 private。



2. 配置步骤

1） 默认情况下，iSpirit3026 交换机已经启动了 snmp ，所以设置 snmp 时，只要设置 snmp community 和相关参数就可以。

Switch# snmp community
Community Name : public
//设置 community 为 public，这个参数是一个字符串，内容不限
View Name(internet) :
 ReadOnly(1),ReadWrite(2)
Permission : 1 //选择 1，将属性设置为只读

Switch# snmp community
Community Name : private
//设置 community 为 private，这个参数是一个字符串，内容不限
View Name(internet) :
 ReadOnly(1),ReadWrite(2)
Permission : 2 //选择 2，将属性设置为为读写。

查看 snmp community 的配置
Switch# show snmp community

CommunityName	ViewName	Permission	Status
public	internet	ReadOnly	Active
private	internet	ReadWrite	Active

如果查看到上述的配置信息。一般就没有问题了。接着就是对管理站进行相关设置。管理站的设置，请查阅管理软件的相关配置手册。

2) 配置了 snmp 之后，还可以进行可选配置，如 trap

trap 指的是当交换机发生特殊情况时，主动向 snmp 管理站发送 snmp 信息。

需要配置 trap 功能，选择 snmp 版本为 2

```
Switch# snmp trap
trap name : test
Target Ip Addr: 192.168.0.100
 snmpv1(1),snmpv2(2),snmpv3(3)
Version : 2
```

查看配置信息：

```
Switch# show snmp trap
- Trap Name             : test
  Transport Domain : 1.3.6.1.6.1.1
  Target ip           : 192.168.0.100
  Target port         : 162
  TimeOut             : 1500
  Retry Count         : 0
  Version             : snmp V2
  Storage Type        : nonvolatile
  Status              : Active
```

3.排错

如果 snmp 不起作用，需要查看以下几个方面：

1) 交换机上需要配置读写或只读的 community ,例如只读为 pubic ,读写为 private,这两个字符串要与管理站上的管理软件设置一致。
2) 同上述类似的问题，也需要在 snmp 服务器上配置同样的 community，才能够使 snmp 服务器对交换机进行远程察看或者管理。
3) 交换上上是否关闭了 snmp。(默认情况是打开 snmp 功能)。可以通过 show manager 查看 snmp 是否打开。关闭 snmp 的命令为： disable snmp；打开则为 enable snmp

如果交换机不能主动发起 trap 信息给 snmp 服务器，需要查看以下：

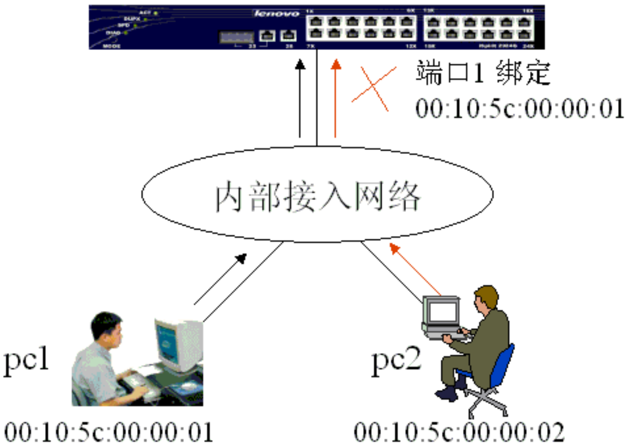
1) 需要在交换机上设置 trap 接收者的 ip 地址，也就是 snmp 服务器的 ip 地址。

确保交换机的 ip 地址和 snmp 服务器之间的 ip 是能够相通的。

十一．MAC 绑定配置

1. 网络需求

某公司想通过 mac 地址来控制接入 iSpirit3026 交换机的用户，只允许 mac 为 00:10:5c:00:00:01 可以通过端口 1 接入网络。拓扑图如下：



2.配置步骤

1) 将 mac 绑定到端口 1

Switch# mac bind **1 1** 00:10:5c:00:00:01 //第一个 1 为端口号，第二个 1 为 vlan 号

2) 查看 mac 绑定信息

Switch# show mac bind

PORT	VLAN	macAddress	STATUS
1	1	00:10:5c:00:00:01	Active

//注意：

*当 mac 地址为 00:10:5c:00:00:01 绑定在端口 1，那么就不能将此 mac 地址绑定到其它端口（在本例中，所有端口都是在 vlan1 里）。**如果 iSpirit3026 划分了多个 vlan，那么同一个 mac 地址可以绑定到不同 vlan 里的端口。**在上述的实例中，端口 1 绑定了 00:10:5c:00:00:01，那么端口 1 就只能允许 mac 地址为 00:10:5c:00:00:01 通过该端口，而且 mac 地址 00:10:5c:00:00:01 是不能通过其它端口进入网络的。iSpirit3026 一个端口最多可以绑定 128 个 mac 地址。*

Mac 地址的绑定方法除了上述的手工绑定之外，还有一种叫自动 mac 绑定。这种使用方法是当交换机学习到 mac 地址之后，使用命令：mac bind 端口号 进行自动绑定。如果端口还没有学习到 mac，那么使用 mac bind 是绑定不到 mac 地址的。采用动态 mac 绑定方法，一个端口最多也是只能绑定 128mac 地址，但每个端口学习到 mac 地址多于 128 个时，那么每个端口只有前 128mac 地址可以在自动绑定方法中被绑定。自动 mac 绑定是在端口没有进行手工 mac 绑定的情况下才可以进行绑定，但是，手工 mac 绑定则不管端口是否进行了自动

绑定，也就端口进行了自动绑定之后，还是可以进行手工 mac 绑定,只要绑定的 mac 地址数不要超过 128 个就可以。

3. 排错

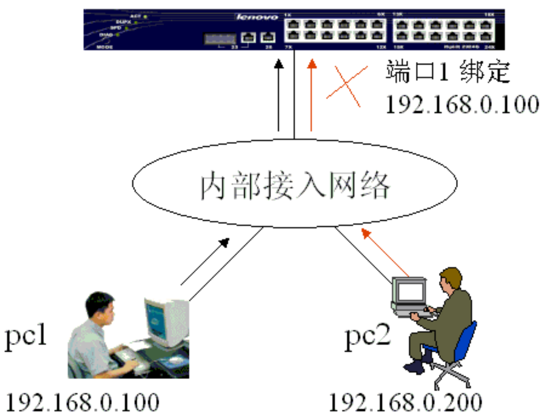
1) 进行 mac 绑定时，如果绑定不成功，那么要检查一下 mac 地址是否正确，是否绑定在正确的端口上。

2) 进行 mac 绑定，要注意 mac 绑定的规则。简单的规则可以参照配置步骤的注意事项。如果想了解更详细的信息，可以查阅 iSpirit3026 用户手册。

十二. IP 绑定配置

1.网络需求

某公司想通过 ip 地址来控制接入 iSpirit3026 交换机的用户，只允许 ip 地址为 192.168.0.100 的用户可以通过端口 1 接入网络。拓扑图如下：



2.配置步骤

1) 将 ip 地址为 192.168.0.100 绑定到端口 1

Switch# ip bind **1** 192.168.0.100 //" 1 "为端口号，这里与 mac 绑定有点不同，没有涉及到 vlan 号

2) 查看端口 1 的 ip 绑定信息

show ip bind 1

port	ipAddress	macAddress
1	192.168.0.100	00:00:00:00:00:00

//注意：

通过以上的配置，可以对端口 1 和 ip 地址为 192.168.0.100 进行控制。端口 1 只能接 ip 地址为 192.168.0.100 的用户。

Ip 绑定与 mac 绑定的规则有点不同。交换机的不同端口可以绑定相同的 ip 地址。如果一个端口 A 绑定了一个 ip 地址，另一个端口 B 没有绑定 ip 地址，那么端口 A 所绑定的 ip 地址的用户是可以通过端口 B 访问网络。一个端口最多可以绑定 127 个 ip 地址。

3.排错

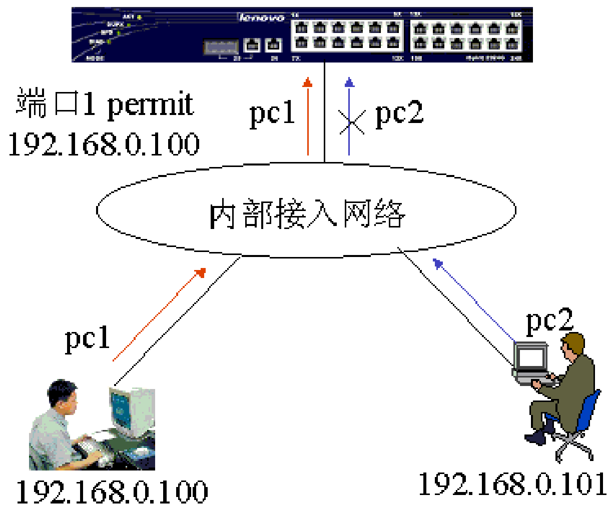
1) 进行 ip 绑定时，如果绑定不成功，那么要检查一下 ip 地址是否正确，是否绑定在正确的端口上。

2) 进行 ip 绑定，要注意 ip 绑定的规则。简单的规则可以参照配置步骤的注意事项。如果想了解更详细的信息，可以查阅 iSpirit3026 用户手册。

十三．ACL 访问控制列表配置

1.标准 IP 规则的 ACL

1）实例：控制交换机端口 1 只能接上 ip 地址为 192.168.0.100 的 pc。如果是其它 ip 地址的 pc 就不能连接到端口 1。也即 ip 地址为 192.168.0.100 的 pc 发出的数据流可以通过交换机的端口 1 转发，而 ip 地址为 192.168.0.101 的 pc 发出的数据流不可以通过交换机的端口 1 转发。



2）配置：

A ：Switch# access-list 1 permit host 192.168.0.100

//默认情况下，在上述列表的规则组 1 之后隐含了一条规则 deny any 的规则，此规则是禁止所有。 一个规则组里可以包含 128 的规则。例如，上述的规则组 1，它除了配置一条规则之外（本例中是 access-list 1 permit host 192.168.0.100 ），还可以配置更多条规则，例如：access-list 1 permit host 192.168.0.123

标准 ip 规则的 acl 的规则组号为 1~199

B:把这标准访问控制列表（access-list 1）应用到 1 端口（对 1 端口流入的数据流做控制）

Switch# port 1

Switch(port 1)# acl-filter 1

//如果没有将访问控制列表应用到端口上，那么此访问控制列表是不起作用的。

在一些使用环境中，如果有多个连续的端口要应用同一个访问控制列表，那么可以一次性

将该访问控制列表应用到多个连续的端口上。例如，要将访问控制列表 100 应用到端口 10—20 上，那么可以进行如下的简单操作：

```
Switch# port 10-20
Switch(port 10-20)#  acl-filter 100
```

3）排错：

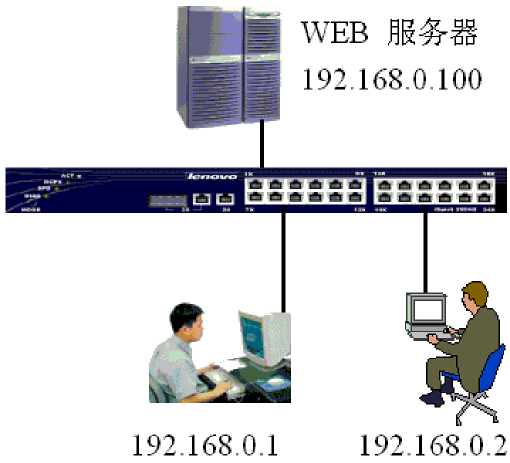
在配置访问控制列表之前确定所有 ip 之间都是通的，然后再添加访问控制列表

这条访问控制列表允许源地址为 192.168.0.100 的 IP 数据流通过交换机。用 show access-list 命令列出访问控制列表进行查看。默认访问控制列表最后都有一条隐含的 deny any 的语句，如果想让其它都通过的话，需要添加一条 permit any 的语句，否则都不能够通过。

```
Switch# show acl-filter
ACL group and Port Configuration Information
module/port              groupId              status
1                         1                  Active

Switch# show access-list 1
 R - RuleId, SI - Source Ip address, DI - Destination Ip address, IT - Ip Type
 SP - Source Port, DP - Destination Port, PT - Protocol Type
 SM - Source MAC address, DM - Destination MAC address, V - VlanId, ST - Status.
 Standard IP access list:
  GroupId 1 :   reference count(1)
 R 1   permit SI 192.168.0.100 Active
```

2.扩展 IP 规则的 acl（web 控制实例）



1） 网络需求：

在这个网络中，web 服务器的 ip 地址为 192.168.0.100（连接端口 24），用户的 ip 地址为 192.168.0.1~192.168.0.20（对应的端口为 1~20）。为了保护服务器的安全，只允许用户对服务器进行 web 访问。

2） 配置步骤：

A. 建一条只允许用户访问服务器的规则：

Switch# access 200 permit tcp 192.168.0.1 0.0.0.255 host 192.168.0.100 www

//扩展 ip 规则的规则组号为 200～399

B.把访问控制列表 200 应用到 1～20 端口，对流入的数据流做控制

Switch# port 1

Switch(port 1)# acl-filter 200

Switch# port 2

Switch(port 1)# acl-filter 200

其它端口的配置与上述类似。

3） 排错：

A 对于特定的应用需要指定特定四层网络端口。而且默认访问控制列表最后都有一条隐含的 deny any 的语句，如果想让其他都通过的话，需要添加一条 permit any 的语句，否则都不能够通过。

B 需要用 show access-list 命令来进行查看访问控制列表配置是否正确

Switch# show acl-filter

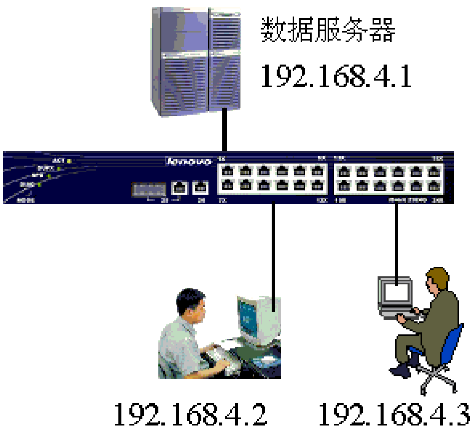
```
ACL group and Port Configuration Information
module/port            groupId           status
  1                     200               Active
  2                     200               Active
```

由于篇幅的限制，这里只以端口 1 和 2 的显示为例。端口 13－24 的显示出的信息应该与上述端口 1 和 2 的信息类似。

C 用 show access-list 命令进行查看

```
Switch# show access
 R - RuleId, SI - Source Ip address, DI - Destination Ip address, IT - Ip Type
 SP - Source Port, DP - Destination Port, PT - Protocol Type
 SM - Source MAC address, DM - Destination MAC address, V - VlanId, ST - Status.
Extended IP access list:
  GroupId 200 : reference count(0)
R 1 permit tcp SI 192.168.0.0 0.0.0.255 DI 192.168.0.100 www Active
```

3.扩展 IP 规则的 acl（单向 ICMP 访问控制实例）



1) 网络环境：

为了防止一般用户刺探网络数据服务器，需要一般用户不能够 PING 通数据服务器，但是数据服务器可以 PING 通其他所有用户。这就需要用到 ICMP 协议号。最好的方法是在连接数据服务器的端口上过滤掉由服务器发出的 ICMP 回应包。这就起到了实现 ICMP 单向访问了。数据服务器连接到 iSpirit3026 交换机的 1 端口

2) 配置步骤：

Switch# access-list 300 deny icmp host 192.168..4.1 any echo-reply
Switch# access-list 300 permit ip any any

并且要把这个访问控制列表应用到 1 端口

Switch# port 1
Switch(port 1)# acl-filter 300
Switch# show access-list 300

R - RuleId, SI - Source Ip address, DI - Destination Ip address, IT - Ip Type
SP - Source Port, DP - Destination Port, PT - Protocol Type
SM - Source MAC address, DM - Destination MAC address, V - VlanId, ST - Status.

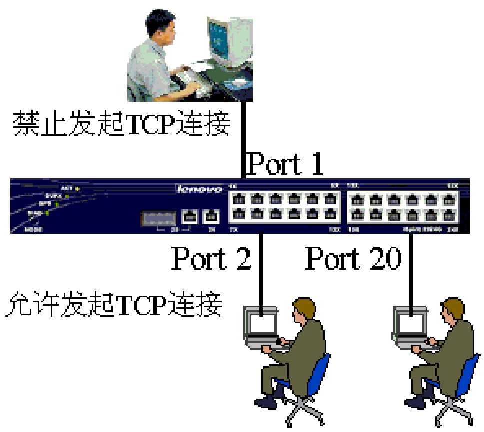
Extended IP access list:
GroupId 300 : reference count(1)
R 1 deny icmp SI 192.168.4.1 DI any echo-reply Active
R 2 permit SI any DI any Active

Switch# show acl-filter

ACL group and Port Configuration Information

port	groupId	status
1	300	Active

4.扩展 IP 规则的 acl（单向 TCP 连接访问控制实例）



1) 网络环境：

为了防止一般网络用户主动连接到重要部门的网络，而仅仅允许重要部门可以主动发起到一般网络用户的联接，这就需要用到单向 TCP 连接。最好的方法是在连接一般网络用户的端口上过滤掉由一般用户发起的 TCP 连接。（本案例中，假设一般用户的网络连接到 iSpirit3026 交换机的 1 端口，重要部门的用户连接到其它端口）

2) 配置步骤：

```
Switch# access-list 200 deny tcp any any 0 syn 1 ack 0
Switch# access-list 200 permit ip any any
```

并且要把这个访问控制列表应用到 1 端口

```
Switch# port 1
Switch(port 1)# acl-filter 200
```

3) 查看配置信息

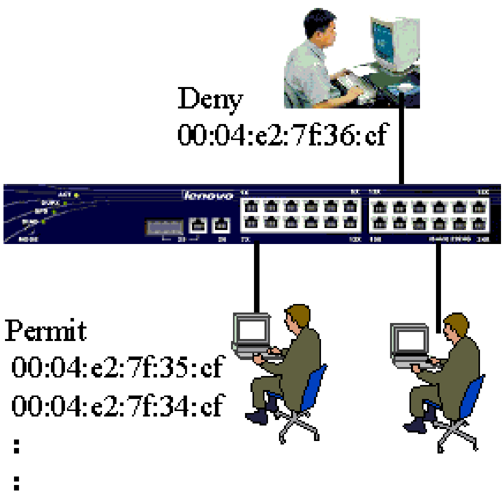
```
Switch# show access-list
 R - RuleId, SI - Source Ip address, DI - Destination Ip address, IT - Ip Type
 SP - Source Port, DP - Destination Port, PT - Protocol Type
 SM - Source MAC address, DM - Destination MAC address, V - VlanId, ST - Status.
 Extended IP access list:
  GroupId 200 : reference count(1)
   R 1 deny tcp SI any DI any syn 1 ack 0 Active
   R 2 permit SI any DI any Active

Switch# show acl-filter
ACL group and Port Configuration Information
port              groupId              status
1                 200                  Active
```

5.MAC 地址规则的访问控制列表

1) 网络需求：

基于安全的考虑，控制特定的 mac 地址为 00:04:e2:7f:36:cf 的特定用户（本例中用户连接到 iSpirit3026 的 1 端口）的数据流不能通过交换机进行转发，而允许其它 mac 地址的数据流通过。



2) 配置步骤：

A．建访问控制列表

Switch# access-list 400 deny 0 ip 00:04:e2:7f:36:cf

Switch# access-list 400 permit 0 ip any

B. 把访问控制列表应用到 iSpirit3026 的 1 端口上对流入的数据流做控制

Switch# port 1

Switch(port 1)# acl-filter 400

C.查看配置信息

Switch# show acl-filter

ACL group and Port Configuration Information

module/port	groupId	status
1	400	Active

Switch# show access-list 400

R - RuleId, SI - Source Ip address, DI - Destination Ip address, IT - Ip Type
SP - Source Port, DP - Destination Port, PT - Protocol Type
SM - Source MAC address, DM - Destination MAC address, V - VlanId, ST - Status.

MAC address list:
GroupId 400 : reference count(0)

```
R 1 deny ip SM 00:04:e2:7f:36:cf DM any Active
R 2 permit ip SM any DM any Active
```

3) 排错：

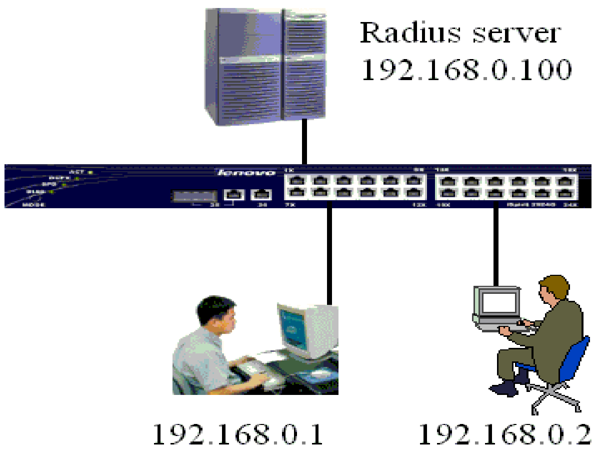
在配置访问控制列表之前确定所有 ip 之间都是通的，然后再添加访问控制列表。还需要用 show access-list 命令来进行查看访问控制列表配置是否正确。

注意 mac 地址一定要书写正确，否则将不起任何作用。而且默认访问控制列表最后都有一条隐含的 deny any 的语句，如果想让其他都通过的话，需要添加一条 permit any 的语句，否则都不能够通过。

十四. 802.1x 认证

1. 网络需求

iSpirit3026 交换机放置了 radius 服务器，ip 地址为 192.168.0.100，子网掩码为 255.255.255.0；用户的 ip 地址为 192.168.0.1 ～ 192.168.0.20，子网掩码为 255.255.255.0。为了控制非法用户使用网络，需要在 iSpirit3026 交换机上打开 802.1x 认证机制，在用户使用的 pc 机上安装 802.1x 客户端，用户只有输入正确的用户名和密码并通过 radius 服务器认证，才能访问网络，用户的数据才能被交换机进行路由和转发。网络拓扑图如下：



2.配置步骤

1) 在全局模式下打开 802.1x 的认证进程，

Switch# dot1x

2) 打开特定端口为 802.1x 的认证端口，本例以端口 1 为例子。

Switch# dot1x control auto 1 // 1 为端口号，如果还有其它端口要对接入的用户进行 802.1x 的认证，那么只要在这个命令上改一下端口号就可以。

3) 指定 radius 服务器的 ip 地址

Switch# radius-server host 192.168.0.100

4) 配置和 radius 服务器相匹配的认证密匙。根据实际情况要和 radius 所配置的一致

Switch# radius-server key radiuslenovonetworks

5) 查看 802.1x 是否配置正确

Switch# show dot1x

Global 802.1X Parameters

Dot1x Status : **Enable** //全局模式下，已经启用了 802.x 认证

```
ReAuth-enabled      :    no
Accounting-enabled  :    yes
ReAuth-period       :    3600
Quiet-period        :    60
Tx-period           :    30
Supp-timeout        :    30
Server-timeout      :    10
Max-req             :    3
reAuthMax           :    3
transmit ports      :

802.1X Port Summary
PortName   Status      Mode    HostNum
1          Link Down   auto    100      //本例中，已经在端口 1 启用 802.1x 认证
2          Link Down   n/a     100
3          Link Down   n/a     100
```

查看 1 端口的状态

```
Switch# show dot1x 1
Port-control              : auto
Maximum hosts             : 100
Current Connecting hosts : 0
```

查看所配置的 radius 服务器是否正确

```
Switch# show radius-server
PrimaryServerIp   : 192.168.0.100
OptionServerIp    : 0.0.0.0
UdpPort           : 1812
accountingPort    : 1813
ShareKey          : radiuslenovonetworks
Vendor            :
NasPort           : 0xc353
NasPortType       : 0x0f
NasPortServer     : 0x02
```

3.排错

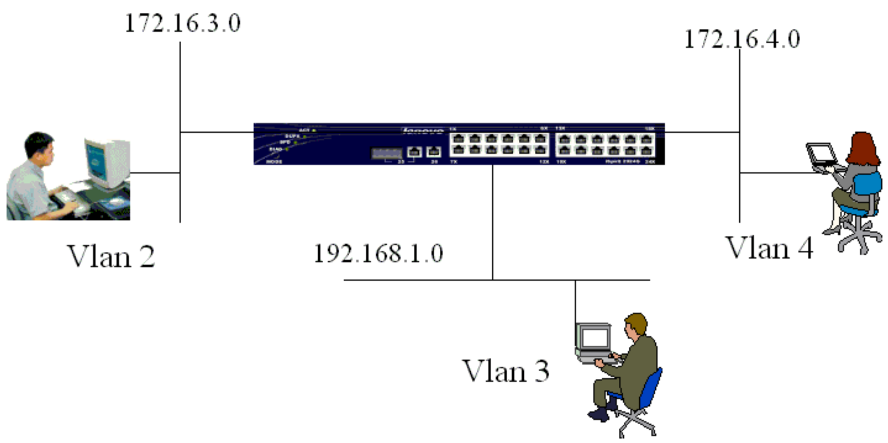
1) 确认一定要打开 802.1x 的认证进程，用 show dot1x 命令
2) 确认打开特定的交换机端口做为认证端口，用 show dot1x 端口号
3) 正确配置 radius 服务器的 ip 地址和认证密钥，用 show radius-server 命令查看

十五. 子网配置

1.网络需求

在 iSpirit3026 创建了三个 vlan，每个 vlan 都有一个管理员，为了使每个管理员都可以管理该交换机，可以通过给每个 vlan 设置一个 ip 地址来实现。交换机详细配置信息

vlan 2 的子网接口为 172.16.3.1　　子网掩码：255.255.255.0
vlan 3 的子网接口为 192.168.1.1　　子网掩码：255.255.255.0
vlan 4 的子网接口为 172.16.4.1　　子网掩码：255.255.255.0
网络拓扑图如下：



2. 配置步骤

1) 在交换机上配置三个 vlan ：vlan2　vlan 3　vlan 4

```
Switch# vlan 2
 Vlan 2 added
Switch(vlan-2)# exit
Switch# vlan 3
 Vlan 3 added
Switch(vlan-3)# exit
Switch# vlan 4
 Vlan 4 added
```

2) 查看 vlan 的配置信息

```
Switch# show vlan
------------------------------------------------
|VID |Name                              | Status |
|----+--------------------------------+--------|
|1    |Default VLAN 1                    | Static |
```

```
|---------------------------------------------|
|2     |vlan2                      | Static |
|---------------------------------------------|
|3     |vlan3                      | Static |
|---------------------------------------------|
|4     |vlan4                      | Static |
|---------------------------------------------|
```

3) 根据实际情况的需求在每个 vlan 内添加交换机的端口

例如，将端口 1 添加到 vlan 2

```
Switch# vlan 2
Switch(vlan-2)# port 1
```

4) 配置交换机的子网

```
Switch# interface vlan 2
switch(interface-vlan2)# ip address 172.16.3.1 255.255.255.0
switch(interface-vlan2)#exit

Switch# interface vlan 3
switch(interface-vlan3)# ip address 192.168.1.1 255.255.255.0
switch(interface-vlan3)#exit

Switch# interface vlan 4
switch(interface-vlan4)# ip address 172.16.4.1 255.255.255.0
switch(interface-vlan4)#exit
```

5)查看配置子网的结果

```
Switch# show ip route
```

ROUTE TABLE

Destination	Netmask	Gateway	Interface	Protocol
172.16.3.0	255.255.255.0	172.16.3.1	vlan2	local
172.16.4.0	255.255.255.0	172.16.4.1	vlan4	local
192.168.0.0	255.255.255.0	192.168.0.1	vlan1	local
192.168.1.0	255.255.255.0	192.168.1.1	vlan3	local

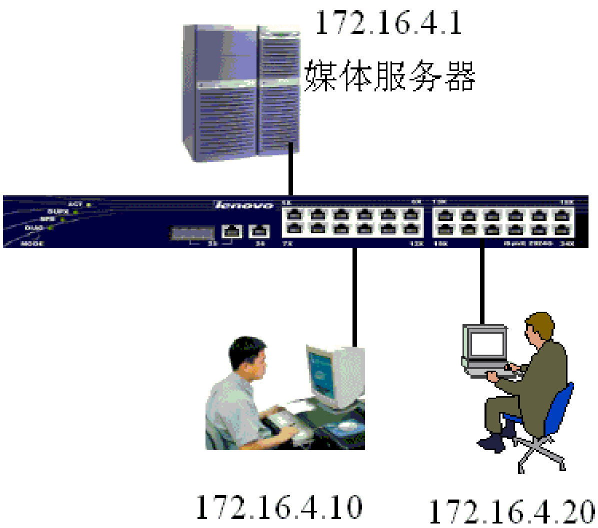
//注意：

通过以上的配置，在 vlan2，3，4 的管理员都可以通过 172.16.3.1，172.16.4.1 或者 192.168.1.1 访问交换机。但是，vlan 2，vlan3，vlan4 里的成员是不能相关访问的。

十六．二层静态组播

1.网络需求

有一个组播服务器 IP 地址为 172.16.4.1 ，在 VLAN1 内，发出组播服务的组播 IP 为 224.100.100.240，也就是二层组播 MAC 01:00:5e:64:64:f0；用户 1 和用户 2 连接到 iSpirit3026 的 1 和 2 端口，并且需要组播服务的话。拓扑图如下：



2.配置步骤

1) 将端口 1-2 加入到组播 01:00:5e:64:64:f0 中
switch# multicast 1 01:00:5e:64:64:f0   1-2

2) 查看配置信息
Switch# show multicast static
multicast address: 01:00:5e:64:64:f0
vlan id: 1
port list: 1 2

十七. 密码恢复

当忘记 iSpirit3026 的密码，可以通过以下方法来解决。

1) 通过超级终端连接到交换机后，重启交换机，注意观察刚启动后从超级终端显示的信息（交换机启动后，很快就可以见到以下的信息）

Lenovo System Boot

Copyright 2001-2003 LegendNetworks Systems, Inc.

CPU: Motorola - MPC8241
Version: iSpirit3026 1.0
Creation date: Apr 8 2004, 15:30:38

Press any key to stop auto-boot...
3 // 特别注意这两行信息，这是一个 3 秒钟的倒计时，在这个倒计时内，在键盘上按任意一键，使交换机进而 boot rom 模式

2) 以下是进入 boot rom 后的信息

[Switch Boot]:

3) 在[Switch Boot]: 模式下，输入“ E1 ”，删除配置文件。请特别注意，“ E1 ”中的“ E ”要大写

例如：[Switch Boot]: E1

4) 输入 E1 之后，出现以下的信息：

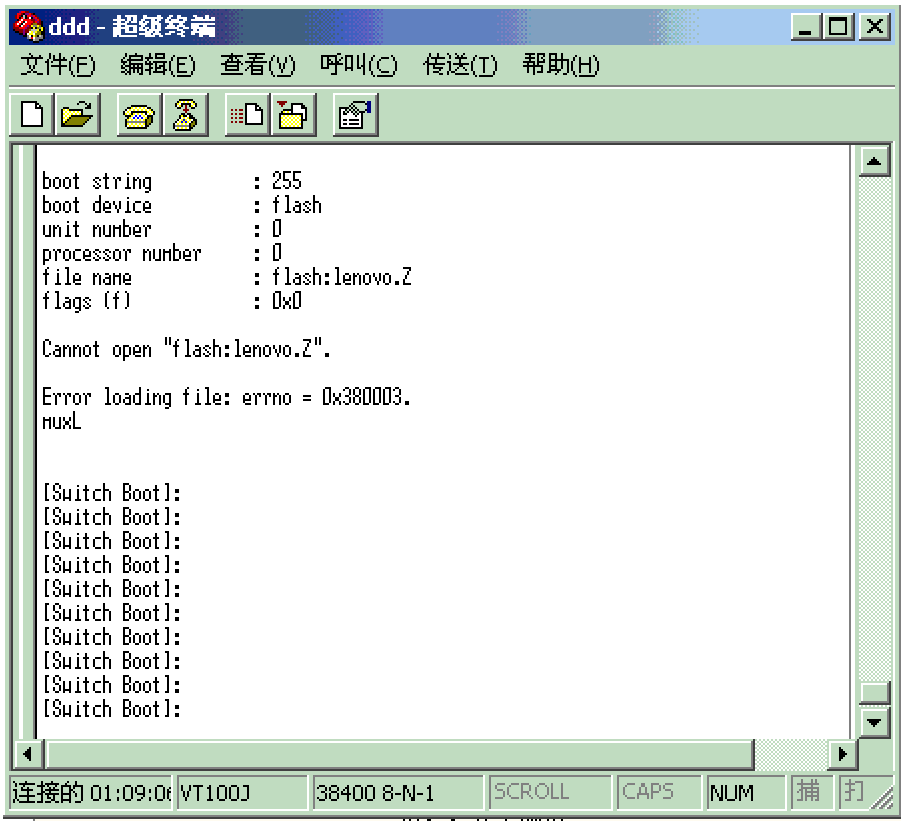
[Switch Boot]: E1
flashDiag: Testing device 4, base: 0xfff80000, 8 sectors @ 64 kB = 512 kB
flashDiag: Erasing
flashDiag: Write sector 0
flashDiag: Write sector 1
flashDiag: Write sector 2

flashDiag: Erasing
flashDiag: Device 4 passed
flashDiagNvRam: Passed
flash cleared
[Switch Boot]:

5) 输入 E1 之后，稍等片刻，即完成上述的操作，当再次出现[Switch Boot]: 输入“ @ ”，使交换机重启动。这时交换机启动后就没有密码。

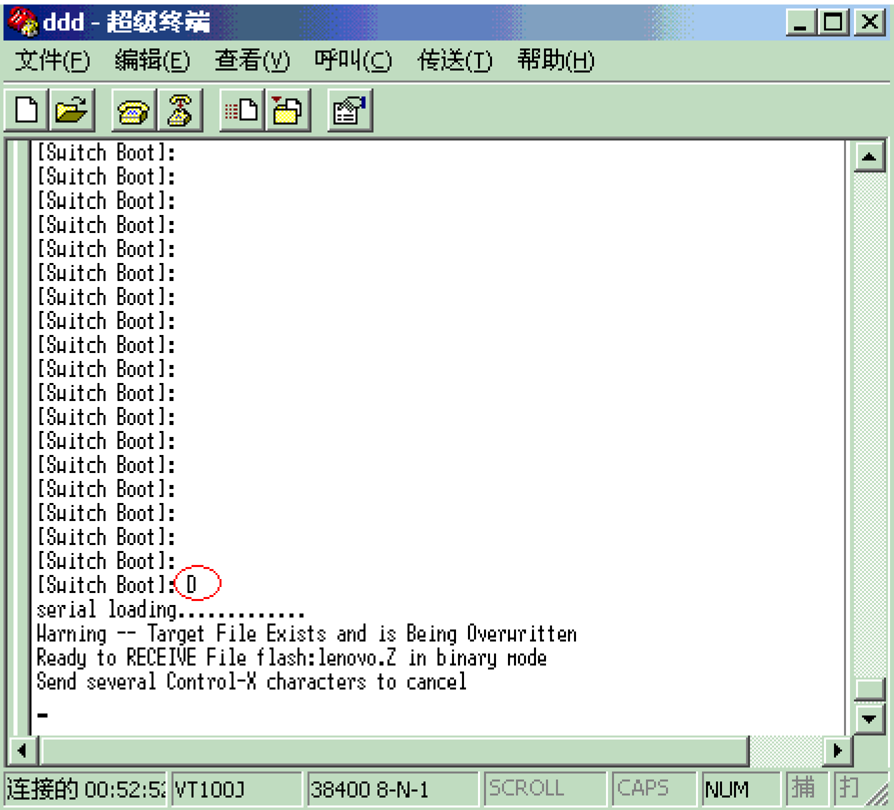
十八. 交换机映像文件损坏的处理方法

交换机一加电后，就出现如下界面，提示出错，而且输入“ @ ”，还是一样情况出现下面的信息，那么很可能是映像文件损坏或者找不到映像文件。



这时可以通过 X modem 协议在 boot rom 下来加载映像文件。具体操作步骤：

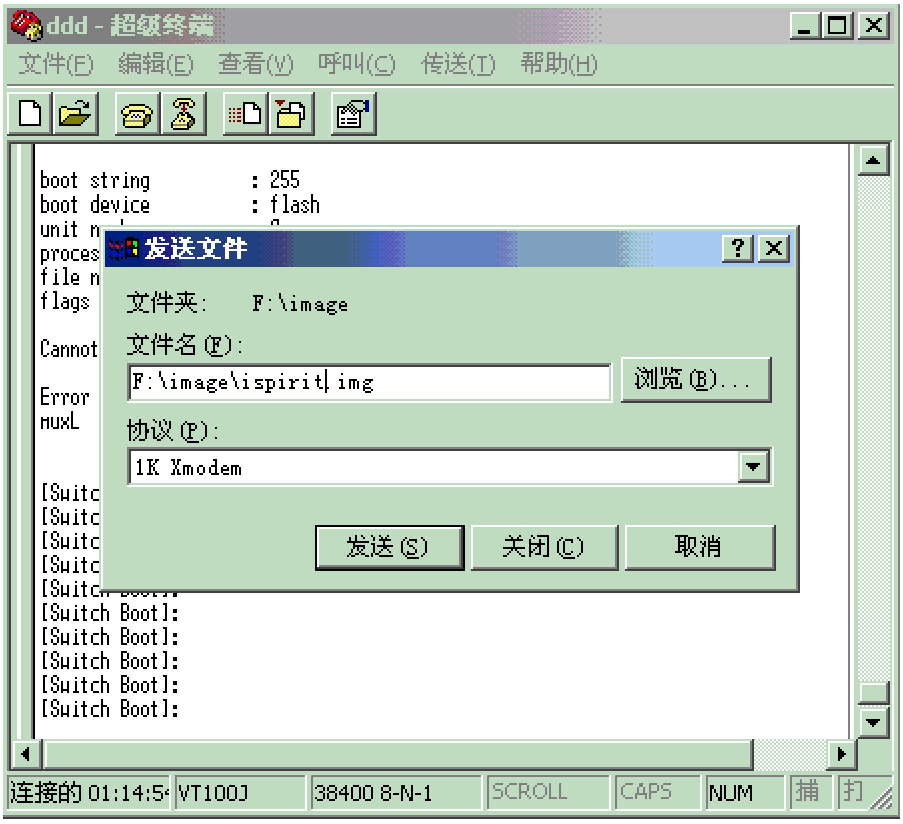
1) 在 boot rom 模式下，输入大小字母“ D ”；



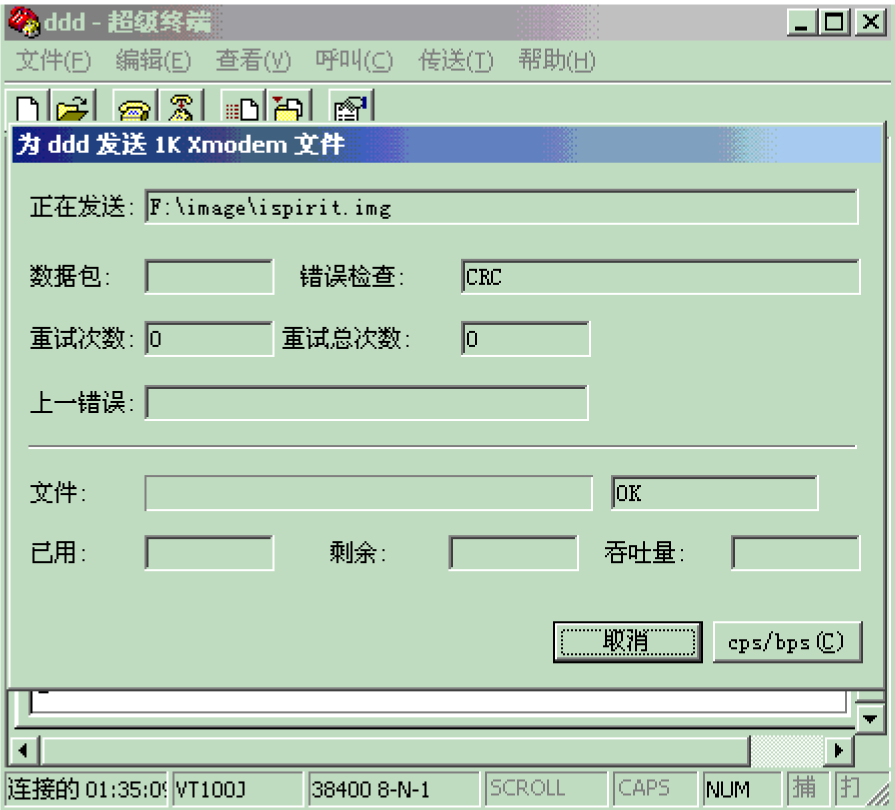
2) 在超级终端处点击“传送”———“发送文件”



3) 在“发送文件”窗口中，点击“浏览”指定升级文件所在的位置，协议选择“1K Xmodem”



4)点击 " 发送 "，出现如下界面，开始正式发送升级文件



5)当文件发送完毕后，出现如下界面，提示发送成功



6) 发送成功后，在[Switch Boot]：处输入 @ ，重启交换机，使交换机进入正常状态。如：swtich>

附件：配置超级终端

1) 将交换机背后的串口与计算机的串口（com1/com2）用串口线连接起来。
2) 打开计算机按照图 1 打开超级终端



图 1 打开超级终端

3) 按图 2，3， 4 配置超级终端


新建连接 - 超级终端
文件(F) 编辑(E) 查看(V) 呼叫(C) 传送(T) 帮助(H)
连接描述
新建连接
输入名称并为该连接选择图标：
名称(N)：
test
图标(I)：
MCI
确定
取消
断开
自动检测
自动检测
SCROLL
CAPS
NUM
捕
打

图 2

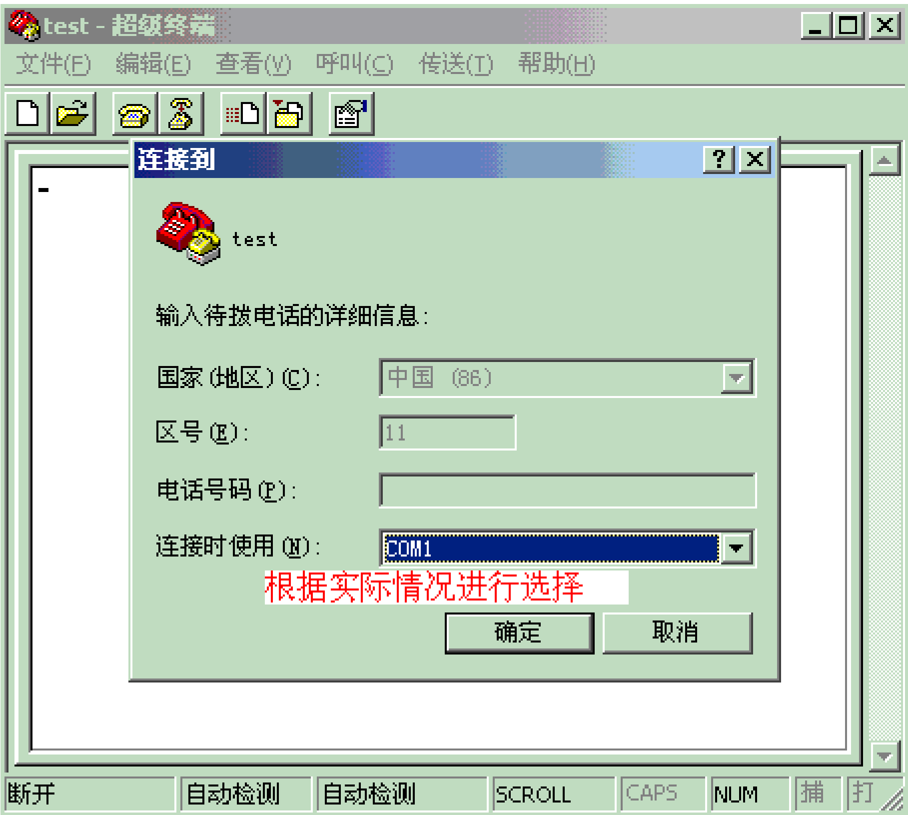

test - 超级终端
文件(F) 编辑(E) 查看(V) 呼叫(C) 传送(T) 帮助(H)
连接到
test
输入待拨电话的详细信息：
国家(地区)(C)：
中国 (86)
区号(E)：
11
电话号码(P)：
连接时使用(N)：
COM1
根据实际情况进行选择
确定
取消
断开
自动检测
自动检测
SCROLL
CAPS
NUM
捕
打

图 3

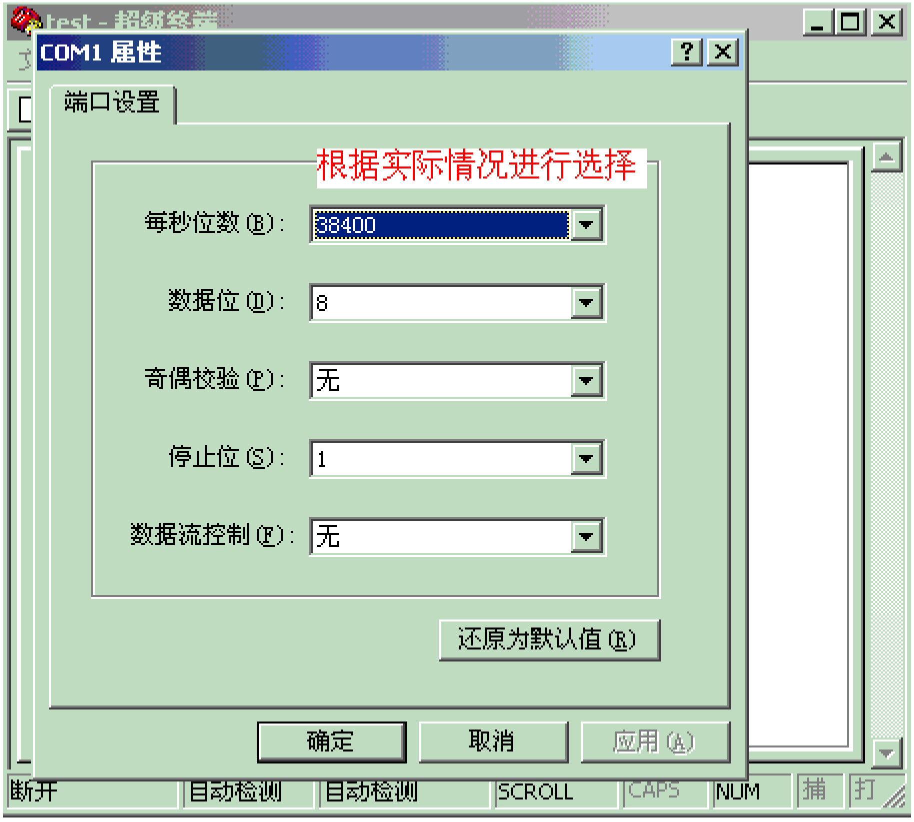


图 4

4) 点击确定，就可以连接到交换机的 CLI 管理界面。